Presentation to the
Crypto-Module Validation Program
2002 Conference

March 27, 2002

ISS Command Security

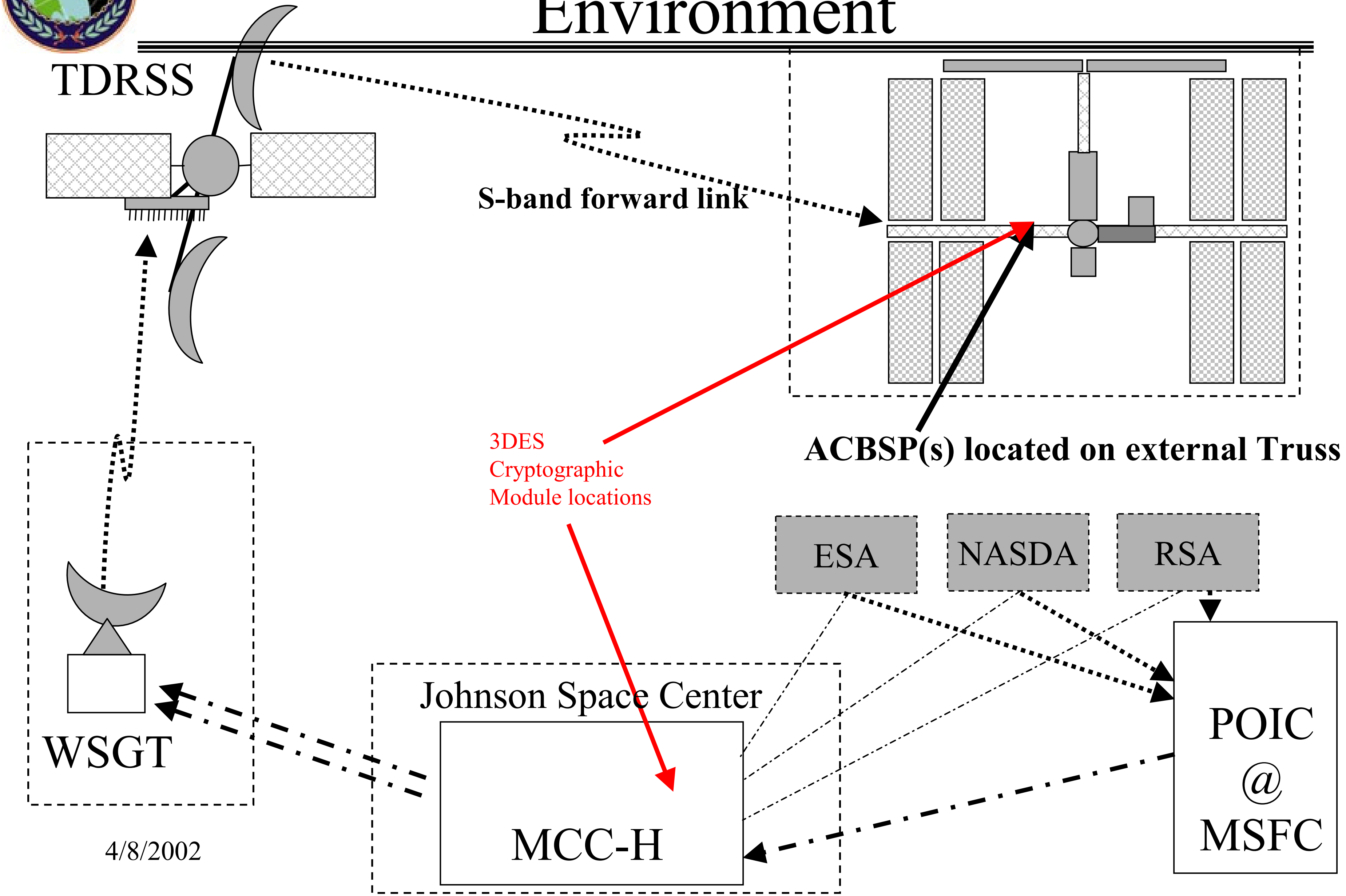
Frederic Stillwagen
NASA Langley Research Center
Spacecraft & Sensors Branch
(757)864-9061
f.h.stillwagen@larc.nasa.gov

Securing ISS Commands

- Command protection in a Space Environment
  - ISS S-band command link communications is transitioning from DES to Triple DES
  - Onboard (ACBSPs) units used for command reception protection and routing
  - Ground (in MCC) units used for command protection formatting and forward link communications

- FIPS 140-2
  - Requirements for CM Validation
  - Applicability with ISS

Command protection in a Space Environment



4/8/2002

Command protection in a Space Environment

- Physical security
  - ACBSP located outside on external truss;
    - Space rated enclosure -- seals and connections;
    - Connects to internal Command & Control Processors (C&C MDMs);
    - EVA access for R&R ONLY;
  - Limited/restricted access while on ground -- unit(s) tracking and reporting
  - MCC unit location in a restricted and access limited facility at NASA JSC
- Environmental Security
  - Space Station Program controls and testing;
  - Stringent environmental testing on ground;
  - Very tight requirements specifications;
  - Lengthy end-to-end testing
  - Ground unit in a controlled and access limited environment
- Command security
  - Triple Data Encryption Standard

FIPS 140-2 CM Validation requirements

- Maximum level required for ISS: Level 2 (ACBSP)
  - Cryptographic Module Specifications - meets requirement
  - **Cryptographic Module Ports and Interfaces**
  - **Roles, Services and Authentication -** Stringent command authentication
  - Finite State Model - meets requirement
  - **Physical Security -** Space rated enclosure, external truss location
  - **Operational environment -** ACBSP location is non-modifiable
  - **Cryptographic Key Management -** ISS Program is a function of agency(s) coordination and extensive key management expertise
  - **EMI/EMC -** Space testing exceeds these levels
  - Self-tests - meets requirement
  - **Design Assurance -** Extensive unit tracking and end-to-end testing; routine training
  - **Mitigation of other attacks -** Design and testing processes

RED indicates Space Station program *'exceeds'* Level 2 requirements by methods of design, testing, Key generation & management methodology

FIPS 140-2 CM Validation requirements

- Maximum level required for ISS: Level 2 (MCC Unit)
  - Cryptographic Module Specifications - meets requirement
  - Cryptographic Module Ports and Interfaces - meets requirement
  - **Roles, Services and Authentication** - Stringent command authentication
  - Finite State Model - meets requirement
  - **Physical Security** - Restricted location and rack mounted enclosure
  - Operational environment - meets requirements
  - **Cryptographic Key Management** - ISS Program is a function of agency(s) coordination and extensive key management expertise
  - EMI/EMC - meets requirement
  - Self-tests - meets requirement
  - Design Assurance - meets requirement
  - **Mitigation of other attacks -** Design and testing processes

RED indicates Space Station program *'exceeds'* Level 2 requirements by methods of design, testing, Key generation & management methodology

ISS Applicability

- ISS will use CMVP to verify and validate on-board and ground cryptographic modules for S-band command communications
- FIPS 140-2 requirements are sometimes exceeded by nature of design for space qualified operation
- ISS Program Command Authentication processes and 3DES CM use provides secure commanding for the life of the Station

Request: Would like to see FIPS 140-2 updated to include applicability to Cryptographic Modules used in a space rated environment

  – Modified or additional security requirement levels

Contacts

Frederic Stillwagen
Aerospace Technologist - telemetry and tracking systems/security Engineer
NASA Langley Research Center
ASCAC - Spacecraft and Sensors Branch
(757)864-9061 ph.
f.h.stillwagen@larc.nasa.gov